"DIRTY" AMENDMENT

Computer Apparatus/Software Access Right Management

This is a continuation-in-part of patent application serial no. :08/587,448, filed on 12/01/95, which is still pending.

Field of the invention

The present invention relates to protection of software/data processing apparatus, and particularly, to protection of [software] them against unauthorised/illegitimate use [or copying].

Background of the invention

Conventionally, [software protection] methods for protecting commercial software products such as programs, multimedia software, distributed through a communication network, such as a telephone system, require a user computer to have a piece of hardware comprising decryption keys and system be installed therein, for to be authenticated by a software program running on the computer. Hardware, rather than software, are being used because software duplication facilities are commonly found in personal computers. However, this is extremely cumbersome and places a large burden on users and vendors alike.

It is therefore an object of the present invention to provide a piece of software to replace the above-mentioned piece of hardware and the rightful user of that piece of software is being discouraged from copying it to someone else, by means of a psychological barrier.

It is therefore another object of the present invention [is] to provide a method to discourage a rightful user from copying his software to someone else by means of a psychological barrier .

It is therefore a further object of the present invention to provide a method to verify the identity of a user of data processing apparatus .

Summary of the invention

According to a first embodiment of the present invention, there is provided a central program comprising 1) a sub-program for providing an Encrypted Identity (herein below referred to as EI sub-program), 2) a sub-program for authorising use of a software [product](herein below referred to as AS sub-program), 3)a sub-program for authenticating user computer (herein below referred to as AC sub-program).

The central program is for managing the use of the individual sub-programs therein so that the AS sub-program can be protected from being accessed directly, thereby preventing it from being copied individually. The EI sub-program is for providing identity information(an encrypted identity) of its rightful owner for accessing a network central computer to obtain services or software products or alike in which a secure operation on a user account of that owner for payment therefor involved. The AC sub-program is for authenticating the computer on which it runs as being a particular predetermined computer, by determining the hardware and software configuration as well as hardware characteristics of that computer by software means and comparing the result with that required. The AS sub-program is for using the authentication result of the AC sub-program and the existence of the EI sub-program which being not protected against unauthorised use and being capable of being used by any user thereof, on a computer, as preconditions for authorising those software [products] which may be purchased commercial computer software obtained to be used on that computer.

It should be noted that in the central program, as far as protection of the software products from being unlawfully copied by the rightful user to someone else is concerned, the AS sub-program is the only sub-program which needs protection and according to the present invention, the AS sub-program is protected from being unauthorised copied by its rightful user to someone else lies on the fact that a rightful user would not copy a software, i.e., the central program in which the EI sub-program exists and which can be used by an unauthorised user to provide the rightful user's

identity information for using the rightful user's account in obtaining, for e.g., network services or software products, to someone else. As seen from the use of automatic teller machine(ATM) magnetic cards, which although can readily be forged, has been proved to be remarkably secure.

According to a second embodiment of the present invention, the central program comprising the EI sub-program only, and the AS sub-program become an individual program which authorises the software product(s) to be used only when the EI sub-program exists in the same computer it runs and which is being determined by receiving an encrypted identity of the EI sub-program from the same.

According to a third embodiment, the EI and AS sub-programs are basically equivalent such that copying the AS sub-program by its rightful user to someone else is equivalent to copying the EI sub-program to someone else, thereby preventing the AS sub-program from unauthorised copying or use.

Brief description of drawings

FIG.1 is a block diagram of the central program.

FIG.2 is a diagrammatic view of a program in which a part B thereof being encrypted, in RAM space.

Detailed description of the preferred embodiments

One object of the [The] present invention is [directed] to [protecting] protect software product(s) distributed through a communication network, against unauthorised copying or use, and for the sake of simplicity, the following description is directed to protection of such software product(s) stored in a user's IBM PC computer. And, the first embodiment of the present invention will be described under the following headings:

1) The Central Program.

2) The Sub-program for providing an Encrypted Identity (EI sub-program).

3) The Sub-program for authorising use of a software product (AS sub-program).

19. (Third time Amended)A method for protecting software from unauthorised use, as claimed by claim 18, wherein no charge [by said software distribution system] for repeating at least said steps c) to e) .

CLEAN AMENDMENT

This is a continuation-in-part of patent application serial no. :08/587,448, filed on 12/01/95, which is still pending.

Field of the invention

The present invention relates to protection of software/data processing apparatus, and particularly, to protection of them against unauthorised/illegitimate use .

Background of the invention

Conventionally, methods for protecting commercial software products such as programs, multimedia software, distributed through a communication network, such as a telephone system, require a user computer to have a piece of hardware comprising decryption keys and system be installed therein, for to be authenticated by a software program running on the computer. Hardware, rather than software, are being used because software duplication facilities are commonly found in personal computers. However, this is extremely cumbersome and places a large burden on users and vendors alike.

It is therefore an object of the present invention to provide a piece of software to replace the above-mentioned piece of hardware and the rightful user of that piece of software is being discouraged from copying it to someone else, by means of a psychological barrier.

It is therefore another object of the present invention to provide a method to discourage a rightful user from copying his software to someone else by means of a psychological barrier .

It is therefore a further object of the present invention to provide a method to verify the identity of a user of data processing apparatus .

Summary of the invention

According to a first embodiment of the present invention, there is provided a central program comprising 1) a sub-program for providing an Encrypted Identity (herein below referred to as EI sub-program), 2) a sub-program for authorising use of a software (herein below referred to as AS sub-program), 3)a sub-program for authenticating user computer (herein below referred to as AC sub-program).

The central program is for managing the use of the individual sub-programs therein so that the AS sub-program can be protected from being accessed directly, thereby preventing it from being copied individually. The EI sub-program is for providing identity information(an encrypted identity) of its rightful owner for accessing a network central computer to obtain services or software products or alike in which a secure operation on a user account of that owner for payment therefor involved. The AC sub-program is for authenticating the computer on which it runs as being a particular predetermined computer, by determining the hardware and software configuration as well as hardware characteristics of that computer by software means and comparing the result with that required. The AS sub-program is for using the authentication result of the AC sub-program and the existence of the EI sub-program which being not protected against unauthorised use and being capable of being used by any user thereof, on a computer, as preconditions for authorising those software which may be purchased commercial computer software obtained to be used on that computer.

It should be noted that in the central program, as far as protection of the software products from being unlawfully copied by the rightful user to someone else is concerned, the AS sub-program is the only sub-program which needs protection and according to the present invention, the AS sub-program is protected from being unauthorised copied by its rightful user to someone else lies on the fact that a rightful user would not copy a software, i.e., the central program in which the EI sub-program exists and which can be used by an unauthorised user to provide the rightful user's

identity information for using the rightful user's account in obtaining, for e.g., network services or software products, to someone else. As seen from the use of automatic teller machine(ATM) magnetic cards, which although can readily be forged, has been proved to be remarkably secure.

According to a second embodiment of the present invention, the central program comprising the EI sub-program only, and the AS sub-program become an individual program which authorises the software product(s) to be used only when the EI sub-program exists in the same computer it runs and which is being determined by receiving an encrypted identity of the EI sub-program from the same.

According to a third embodiment, the EI and AS sub-programs are basically equivalent such that copying the AS sub-program by its rightful user to someone else is equivalent to copying the EI sub-program to someone else, thereby preventing the AS sub-program from unauthorised copying or use.

Brief description of drawings

FIG.1 is a block diagram of the central program.

FIG.2 is a diagrammatic view of a program in which a part B thereof being encrypted, in RAM space.

Detailed description of the preferred embodiments

One object of the present invention is to protect software product(s) distributed through a communication network, against unauthorised copying or use, and for the sake of simplicity, the following description is directed to protection of such software product(s) stored in a user's IBM PC computer. And, the first embodiment of the present invention will be described under the following headings:

1) The Central Program.

2) The Sub-program for providing an Encrypted Identity (EI sub-program).

3) The Sub-program for authorising use of a software product (AS sub-program).

19. A method for protecting software from unauthorised use, as claimed by claim 18, wherein no charge for repeating at least said steps c) to e) .